Math 357
Expositional homework 07

Assigned: 2024–04–12 (F)
Due: 2024–04–19 (F)

The goal of this homework is to work with elementary theory and examples in galois theory to better understand the essential building blocks.

(a) Let $K : K_0$ be a field extension; and let $\operatorname{Aut}(K : K_0)$ be the automorphisms of K that fix K_0, a group under composition of functions. Let K_i be an intermediate field of $K : K_0$, let H_i be a subgroup of $\operatorname{Aut}(K : K_0)$, and let $\mathcal{F}(H_i)$ denote the fixed field of H_i:

$$\mathcal{F}(H_i) = \{\alpha \in K \mid \forall \sigma \in H_i, \sigma(\alpha) = \alpha\}$$

Prove that the associations

$$K_i \mapsto \operatorname{Aut}(K : K_i) \qquad\qquad H_i \mapsto \mathcal{F}(H_i)$$

are inclusion-reversing, that is, if $K_1 \subseteq K_2$ and $H_1 \subseteq H_2$, then

$$\operatorname{Aut}(K : K_1) \supseteq \operatorname{Aut}(K : K_2) \qquad\qquad \mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$$

(b) Prove Proposition 14.5:[1] Let K_0 be a field, let $f \in K_0[t]$, and let $\tilde{K}_{0,f} : K_0$ be a splitting field for f over K_0. Then

$$\# \operatorname{Aut}(\tilde{K}_{0,f} : K_0) \leqslant [\tilde{K}_{0,f} : K_0]$$

with equality if f is separable. You may take as your starting point our diagram from class (see Classes 35 and 36).

(c) Let $\alpha = \sqrt{2} + \sqrt{5} \in \mathbf{C}$.

(i) Find the minimal polynomial $m_{\alpha,\mathbf{Q}}$ for α over $\mathbf{Q}$.

(ii) Prove that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt{5})$.

(iii) Prove that $m_{\alpha,\mathbf{Q}}$ splits completely in $\mathbf{Q}(\alpha)$. *Hint:* Use part (ii).

(iv) Specify all automorphisms in the galois group $\operatorname{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$. State a (more common) group isomorphic to $\operatorname{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$, and draw its subgroup lattice.

(v) Use part (iv) and the fundamental theorem of galois theory to draw the lattice of intermediate fields for $\mathbf{Q}(\alpha) : \mathbf{Q}$.

[1] See DF3e, pp 561–2.

Solution to part (a)

Let $K_1 \subseteq K_2 \subseteq K$, and let $\sigma \in \mathrm{Aut}(K : K_2)$. Then by definition of $\mathrm{Aut}(K : K_2)$, σ is an automorphism of K that fixes K_2; that is, for each $a \in K_2$, $\sigma(a) = a$. Because $K_1 \subseteq K_2$, this shows that σ fixes K_1. Hence $\sigma \in \mathrm{Aut}(K : K_1)$.

Let $H_1 \subseteq H_2 \subseteq \mathrm{Aut}(K : K_0)$, and let $\alpha \in \mathcal{F}(H_2)$. Then by definition of $\mathcal{F}(H_2)$, for all $\sigma \in H_2$, $\sigma(\alpha) = \alpha$. Because $H_1 \subseteq H_2$, this shows that for all $\sigma \in H_1$, $\sigma(\alpha) = \alpha$. Thus $\alpha \in \mathcal{F}(H_1)$.

Solution to part (b)

We sketched a proof together in class. See DF3e, pp 561–562 for a more detailed exposition.

Solution to part (c)

Part (i): One approach is to attempt to "power away" the radicals by successively isolating one radical and raising both sides of the equation to an appropriate power to cancel the radical. Taking this approach, we compute

$$\begin{array}{ccccc} \alpha = \sqrt{2} + \sqrt{5} & \Leftrightarrow & \alpha - \sqrt{5} = \sqrt{2} & \Rightarrow & \alpha^2 - 2\sqrt{5}\alpha + 5 = 2 \\ & \Leftrightarrow & \alpha^2 + 3 = 2\sqrt{5}\alpha & \Rightarrow & \alpha^4 + 6\alpha^2 + 9 = 20\alpha^2 \end{array}$$

so

$$\alpha^4 - 14\alpha^2 + 9 = 0$$

Viewing this equation as a polynomial in $\mathbf{Q}[t]$ evaluated at $t = \alpha$, we define

$$m = t^4 - 14t^2 + 9$$

This polynomial has coefficients in $\mathbf{Q}$ and is monic (by inspection), and it has α as a zero (by construction).

For m to be the minimal polynomial of α over $\mathbf{Q}$, it remains only to show that m is irreducible. To do this, one can show that m has no factors of degree 1 or degree 2, either directly in $\mathbf{Q}$ or in a quotient ring of $\mathbf{Z}$ (for example, $\mathbf{Z}/(5)$. Alternatively, one can use knowledge of the set of zeros of m (see our response to part (iii)) to show that (i) no zero of m is in $\mathbf{Q}$; and (ii) for all distinct zeros α_1, α_2 of m, the degree-2 polynomial $(t - \alpha_1)(t - \alpha_2)$ has a coefficient that is not in $\mathbf{Q}$. Note that with this latter approach, it suffices to check three such products (fix one zero α_1 and let α_2 run through the other three).

Another approach is to implement the technique in exercise (f) on expositional homework 06: Find a matrix representation of the "multiplication by α" map on some finite-degree field extension $K : \mathbf{Q}$ with $\alpha \in K$. This approach requires that we find such an extension (as shown in part (ii), the extension field $K = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ will do) and a basis for K as a $\mathbf{Q}$-vector space. As above, we need to verify that the polynomial we obtain is irreducible. If not, then we need to find an irreducible factor that has α as a zero.

Part (ii): We prove set inclusion in both directions. By definition, $\alpha = \sqrt{2} + \sqrt{5}$, so $\mathbf{Q}(\sqrt{2}, \sqrt{5})$ is a field that contains both $\mathbf{Q}$ and α, and hence it contains the field generated by α over $\mathbf{Q}$: $\mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{5})$. For the reverse inclusion, because $\mathbf{Q}(\alpha)$ is a field, it is closed under field operations: addition, multiplication, and taking additive and multiplicative inverses. In particular, $\mathbf{Q}(\alpha)$ contains

$$\alpha^{-1} = \frac{1}{\sqrt{5}+\sqrt{2}} = \frac{\sqrt{5}-\sqrt{2}}{(\sqrt{5}+\sqrt{2})(\sqrt{5}-\sqrt{2})} = \frac{1}{3}(\sqrt{5}-\sqrt{2})$$

so it also contains

$$3\alpha^{-1} = \sqrt{5}-\sqrt{2}$$

so it also contains

$$\frac{1}{2}(\alpha + 3\alpha^{-1}) = \sqrt{5} \qquad \text{and} \qquad \frac{1}{2}(\alpha - 3\alpha^{-1}) = \sqrt{2}$$

That is, $\mathbf{Q}(\alpha)$ is a field that contains $\mathbf{Q}$ and the elements $\sqrt{2}$ and $\sqrt{5}$, so it contains the field generated by $\{\sqrt{2}, \sqrt{5}\}$ over $\mathbf{Q}$: $\mathbf{Q}(\alpha) \supseteq \mathbf{Q}(\sqrt{2}, \sqrt{5})$.

Part (iii): One can check that the four elements $\pm\sqrt{2} \pm \sqrt{5} \in \mathbf{C}$ are zeros of $m_{\alpha,\mathbf{Q}}$ (which has degree 4, so these are all the zeros) and are distinct. Each element is in $\mathbf{Q}(\sqrt{2}, \sqrt{5}) = \mathbf{Q}(\alpha)$. Therefore, $m_{\alpha,\mathbf{Q}}$ splits completely in $\mathbf{Q}(\alpha)$.

Note that we have shown that $\mathbf{Q}(\alpha) : \mathbf{Q}$ is a splitting field of the separable polynomial $m_{\alpha,\mathbf{Q}} \in \mathbf{Q}[t]$. Thus the field extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is galois.

Part (iv): To specify automorphisms in $\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$, we will find it convenient to use the fact that $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt{5})$, which we proved in part (ii). This equality shows that $\{\sqrt{2}, \sqrt{5}\}$ generates $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$. Therefore, to specify an element σ of $\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$, it suffices to specify the images $\sigma(\sqrt{2})$ and $\sigma(\sqrt{5})$.

The elements $\sqrt{2}$ and $\sqrt{5}$ have minimal polynomials over $\mathbf{Q}$ of

$$m_{\sqrt{2},\mathbf{Q}} = t^2 - 2 \qquad\qquad m_{\sqrt{5},\mathbf{Q}} = t^2 - 5$$

respectively. Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$. The requirement that σ must permute the zeros of any irreducible polynomial gives us four candidate automorphisms:

$$\begin{array}{cccc} \sqrt{2} \mapsto \sqrt{2} & \sqrt{2} \mapsto -\sqrt{2} & \sqrt{2} \mapsto \sqrt{2} & \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{5} \mapsto \sqrt{5} & \sqrt{5} \mapsto \sqrt{5} & \sqrt{5} \mapsto -\sqrt{5} & \sqrt{5} \mapsto -\sqrt{5} \end{array}$$

In part (iii) we showed that the field extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is galois. Therefore

$$\#\,\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q}) = [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg m_{\alpha,\mathbf{Q}} = 4$$

Thus all four candidate automorphisms are indeed automorphisms in $\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$.

Let

$$\tau_2 : \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{5} \mapsto \sqrt{5} \end{array} \qquad\qquad \tau_5 : \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{5} \mapsto -\sqrt{5} \end{array}$$

It is straightforward to check that $\{\tau_2, \tau_5\}$ generate $\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$ and that each automorphism has order 2:

$$\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q}) = \langle \tau_2, \tau_5 \,|\, \tau_2^2, \tau_5^2 \rangle$$

Thus $\mathrm{Gal}(\mathbf{Q}(\alpha) : \mathbf{Q})$ is isomorphic to the Klein four-group. Its subgroup lattice is given in DF3e, p 567. (The automorphisms that we have denoted τ_2 and τ_5 correspond to σ and τ in this diagram.)

Part (v): The subfield lattice (aka lattice of intermediate fields) is given in DF3e, p 568. (Replace $\sqrt{3}$ with $\sqrt{5}$ throughout.) We use the fundamental theorem of galois theory to match subgroup with subfield. For example, let's compute the subfield corresponding to the subgroup

$$H = \langle \tau_2\tau_5 \rangle = \{\mathrm{id}_{\mathbf{Q}(\sqrt{2},\sqrt{5})}, \tau_2\tau_5\}$$

By the fundamental theorem of galois theory, this subfield is $\mathcal{F}(H)$ Let $\beta \in \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ be arbitrary. Because $\{1, \sqrt{2}, \sqrt{5}, \sqrt{2}\sqrt{5}\}$ is a basis for $\mathbf{Q}(\alpha)$ as a $\mathbf{Q}$-vector space, there exist unique $a_{i,j} \in \mathbf{Q}$ such that

$$\beta = a_{0,0}1 + a_{0,1}\sqrt{5} + a_{1,0}\sqrt{2} + a_{1,1}\sqrt{2}\sqrt{5}$$

By definition, $\beta \in \mathcal{F}(H)$ if and only if for all $\sigma \in H$, σ fixes β: $\sigma(\beta) = \beta$. This equation is satisfied for the identity map $\mathrm{id}_{\mathbf{Q}(\sqrt{2},\sqrt{5})}$. The only other element of H is $\tau_2\tau_5$. Using the fact that elements of the galois group are field homomorphisms that fix each element of the base field (here, $\mathbf{Q}$), we compute

$$\begin{aligned}
\tau_2\tau_5(\beta) &= \tau_2\tau_5(a_{0,0}1 + a_{0,1}\sqrt{5} + a_{1,0}\sqrt{2} + a_{1,1}\sqrt{2}\sqrt{5}) \\
&= a_{0,0} \cdot \tau_2\tau_5(1) + a_{0,1} \cdot \tau_2\tau_5(\sqrt{5}) + a_{1,0} \cdot \tau_2\tau_5(\sqrt{2}) + a_{1,1} \cdot \tau_2\tau_5(\sqrt{2}\sqrt{5}) \\
&= a_{0,0}1 - a_{0,1}\sqrt{5} - a_{1,0}\sqrt{2} + a_{1,1}\sqrt{2}\sqrt{5}
\end{aligned}$$

Thus $\beta \in \mathcal{F}(H) = \mathcal{F}(\{\mathrm{id}_{\mathbf{Q}(\sqrt{2},\sqrt{5})}, \tau_2\tau_5\})$ if and only if

$$\tau_2\tau_5(\beta) = \beta \qquad \Leftrightarrow \qquad a_{0,1} = 0 \text{ and } a_{1,0} = 0 \qquad \Leftrightarrow \qquad \beta \in \mathrm{Span}_{\mathbf{Q}}(1, \sqrt{2}\sqrt{5}) = \mathbf{Q}(\sqrt{10})$$